PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-150532
(43)Date of publication of application : 02.06.1999

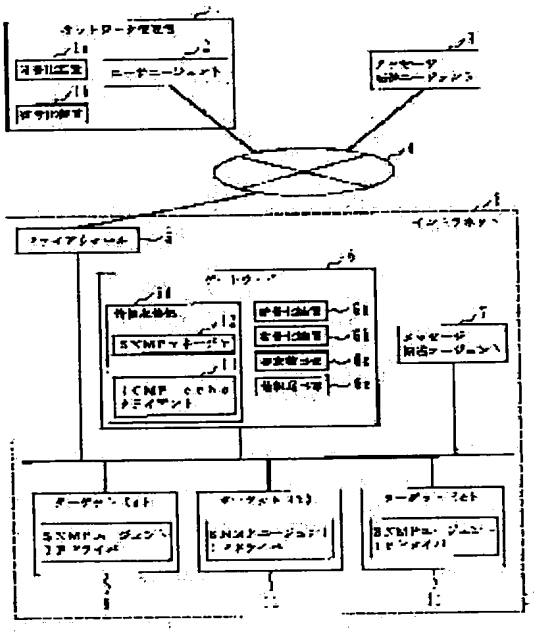
(51)Int.Cl. H04L 12/24
H04L 12/26
G06F 13/00
G06F 13/00
H04L 12/66

(21)Application number : 09-316740
(22)Date of filing : 18.11.1997

(71)Applicant : HITACHI INFORMATION SYSTEMS LTD
(72)Inventor : ABE SHUNSUKE

(54) REMOTE MANAGEMENT SYSTEM FOR INTRA-NET AND STORAGE MEDIUM STORING PROGRAM USED FOR IT

(57)Abstract:
PROBLEM TO BE SOLVED: To provide the remote management system for an intra-net which enables remote management of the intra-net via the internet so as to reduce a network management cost and to provide the storage medium that records a program used for the system.
SOLUTION: A gateway 6 is provided with a request detection section 6c that reads an intra-net management information request from a message in electronic mail sent to the intra-net 8 via the Internet 4, an information collection section 6d that collects the intra-net management information corresponding to the intra-net management information request read, and an information transmission section 6e that returns the collected intra-net management information as a message in electronic mail via the internet 4. The intra-net 8 having a firewall 5 is managed by using the electronic mail via the internet 4.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－150532

(43)公開日　平成11年(1999)６月２日

(51)Int.Cl.[6]		識別記号	FI		
Ｈ０４Ｌ	12/24		Ｈ０４Ｌ	11/08	
	12/26		Ｇ０６Ｆ	13/00	３５１Ｇ
Ｇ０６Ｆ	13/00	３５１			３５３Ｕ
		３５３	Ｈ０４Ｌ	11/20	Ｂ
Ｈ０４Ｌ	12/66				

審査請求　未請求　請求項の数４　ＯＬ　（全９頁）

(21)出願番号　特願平9－316740

(22)出願日　平成９年(1997)11月18日

(71)出願人　000152985
株式会社日立情報システムズ
東京都渋谷区道玄坂１丁目16番５号

(72)発明者　安部　俊輔
東京都渋谷区道玄坂一丁目16番５号　株式会社日立情報システムズ内

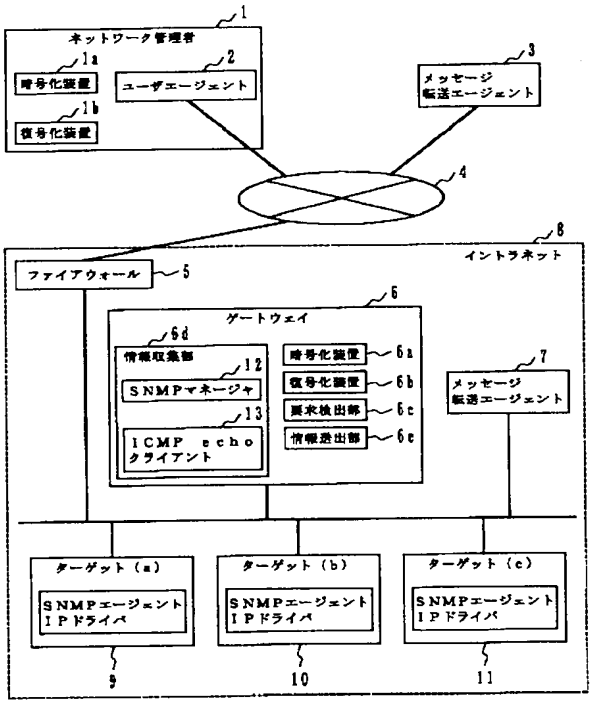
(74)代理人　弁理士　磯村　雅俊　（外１名）

(54)【発明の名称】　イントラネットの遠隔管理システムおよびこれに用いるプログラムを記録した記録媒体

(57)【要約】

【課題】　インターネット経由で、ファイアウォールが設けられたイントラネットの遠隔管理ができない。

【解決手段】　インターネット４経由でイントラネット８に送られてきた電子メール中のメッセージからイントラネットの管理情報要求を読み取る要求検出部６ｃと、読み取ったイントラネットの管理情報要求に対応してイントラネットの管理情報を収集する情報収集部６ｄと、収集したイントラネットの管理情報を電子メール中のメッセージとしてインターネット４経由で返送する情報送出部６ｅとをゲートウェイ６に設け、ファイアウォール５を有するイントラネット８の管理をインターネット４経由で電子メールを用いて行う構成とする。



1

【特許請求の範囲】

【請求項１】　ファイアウォールを介してインターネットと接続されたイントラネットの管理を行うシステムであって、上記インターネット経由で上記イントラネットに送られてきた電子メールを受信し、該電子メール中のメッセージから上記イントラネットの管理情報要求を読み取る第１の手段と、該第１の手段で読み取った上記イントラネットの管理情報要求に対応してイントラネットの管理情報を収集する第２の手段と、該第２の手段で収集したイントラネットの管理情報を電子メール中のメッセージとして上記インターネット経由で返送する第３の手段とを有し、上記ファイアウォールを介して接続されたイントラネットの管理をインターネット経由で電子メールを用いて行うことを特徴とするイントラネットの遠隔管理システム。

【請求項２】　請求項１に記載のイントラネットの遠隔管理システムにおいて、上記第１の手段で読み取る上記電子メール中のメッセージから予め暗号化された上記イントラネットの管理情報要求を復号化する復号化手段と、上記第３の手段で上記電子メール中のメッセージとして返送する上記イントラネットの管理情報を暗号化する暗号化手段とを設け、上記イントラネットの管理情報を暗号化して上記インターネット上に送出することを特徴とするイントラネットの遠隔管理システム。

【請求項３】　請求項２に記載のイントラネットの遠隔管理システムにおいて、上記第１の手段と上記第２の手段および上記第３の手段、ならびに、上記復号化手段と上記暗号化手段を、上記イントラネット上のゲートウェイに設けたことを特徴とするイントラネットの遠隔管理システム。

【請求項４】　ファイアウォールを介してインターネットと接続されたイントラネットの遠隔管理を行うコンピュータで用いるプログラムを記録した記録媒体であって、上記イントラネットの遠隔管理を行うコンピュータに、上記インターネット経由で上記イントラネットに送られてきた電子メールを受信し、該電子メール中のメッセージから上記イントラネットの管理情報要求を読み取る第１の手順と、該第１の手順で読み取った上記イントラネットの管理情報要求に対応してイントラネットの管理情報を収集する第２の手順と、該第２の手順で収集したイントラネットの管理情報を電子メール中のメッセージとして上記インターネット経由で返送する第３の手順とを含み、上記ファイアウォールを介して接続されたイントラネットの遠隔管理をインターネット経由で電子メールを用いて行わせるためのプログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、コンピュータネットワークの遠隔管理技術に係わり、特に、イントラネットの遠隔管理を効率的に行うのに好適なイントラネットの遠隔管理システムおよびこれに用いるプログラムを記録した記録媒体に関するものである。

2

【０００２】

【従来の技術】近年のインターネットの普及により、国や組織の境界を越えてコンピュータ同士の通信が可能になっている。また、イントラネットと呼ばれるインターネットの技術を取り入れて企業内のコンピュータネットワークを構築するケースが増えている。

【０００３】このイントラネットではＴＣＰ／ＩＰ（Transmission Control Protocol/Internet Protocol）をベースとした通信が行われ、例えば、「９７年版　情報・通信新語辞典」（１９９７年、日経ＢＰ社発行）の第５２９～５３０頁に記載のように、ＳＮＭＰ（Simple Network Management Protocol）によるネットワーク管理が行なわれる。

【０００４】従来、遠隔地からイントラネットの管理を行う場合には、専用線やダイアルアップ回線を設置することが行われていた。しかし、専用線は、一定の帯域が保証される一方で、一般的に通信費が高い。また、ダイアルアップ回線は、通常の加入電話回線でモデム同士を接続するものであり、設備は廉価であるが、遠距離市外通話では通信費が割高になるという問題点があった。インターネットを利用すれば、ダイアルアップ回線であってもインターネットサービス提供者のアクセスポイントへの市内通話料のみを負担するだけで良いので通信費の削減に役立つ。

【０００５】しかし、インターネットに接続した各企業では、通常、セキュリティを確保するために、いわゆるファイアウォール（内部のローカルネットワークと外部のインターネットとの間に、外部からの不正なアクセスを防ぐ目的で設置されるコンピュータ）を用いてインターネットからのイントラネットへのパケットの流入を制限している。従って、インターネットからイントラネットの遠隔管理を行おうとしても、ファイアウォールが障害となってイントラネットへのアクセスができない。

【０００６】

【発明が解決しようとする課題】解決しようとする問題点は、従来の技術では、ファイアウォールが障害となってインターネットからイントラネットの遠隔管理アクセスができない点である。本発明の目的は、これら従来技術の課題を解決し、インターネット経由でのイントラネットの遠隔管理を可能とし、ネットワーク管理コストの削減を図ることができるイントラネットの遠隔管理システムおよびこれに用いるプログラムを記録した記録媒体を提供することである。

【０００７】

【課題を解決するための手段】上記目的を達成するため、本発明のイントラネットの遠隔管理システムは、イントラネット中に例えばゲートウェイ（二つのプロトコ

ルを相互に変換するコンピュータ）を設置し、このゲートウェイで、電子メールプロトコル（SMTP: Simple Mail Transfer Protocol)とネットワーク管理プロトコル(SNMP: Simple Network Management Protocol、および、ping：ICMP echo Protocol)とを相互に変換させる構成とする。すなわち、電子メールはファイアウォールを通過することができるので、ネットワーク管理者は、ネットワークの管理情報の取得・設定要求を電子メールの本文中に命令文として記述し、電子メールプロトコル（SMTP）を利用して、イントラネットに送信する。ゲートウェイは電子メールで要求を受信すると、イントラネット上の、管理対象のコンピュータに関する情報を取得あるいは設定し、その実行結果を電子メールの形で、ネットワーク管理者側に返信する。尚、電子メール中のメッセージはインターネット上を通過する際は暗号化することにより、インターネット上の第三者が参照できないようにする。

【０００８】

【発明の実施の形態】以下、本発明の実施例を、図面により詳細に説明する。図１は、本発明のイントラネットの遠隔管理システムの構成の一実施例を示すブロック図である。本図１において、１はネットワーク管理者用のコンピュータ（図中、「ネットワーク管理者」と記載）、２はネットワーク管理者用のコンピュータ１が有するユーザエージェント（ユーザの代わりに電子メールのメッセージを送信・受信するプロセス）、３はネットワーク管理者用のコンピュータ１が利用するメッセージ転送エージェント（電子メールのメッセージを格納あるいは転送するプロセス）、４はインターネット、５はファイアウォール、６はゲートウェイ、７はイントラネット内のメッセージ転送エージェント、８はイントラネット、９～１１はイントラネット８上の管理対象コンピュータ（図中、「ターゲット（ａ）～（ｃ）」と記載）である。

【０００９】メッセージ転送エージェント３は、インターネット４のサービス提供者が管理するコンピュータ上に存在する。ネットワーク管理者用のコンピュータ１とゲートウェイ６は、それぞれ、暗号化装置１ａ，６ａと復号化装置１ｂ，６ｂを有し、電子メールの内容の暗号化・復号化と、暗号・復号キーの生成を行う。

【００１０】尚、第三者が傍受したメッセージを再送信することによる攻撃に対する防御のため、暗号化・復号化キーは１回の通信毎に一方向ハッシュ関数を適用して更新されるものとする。また、暗号化アルゴリズムは、対照型アルゴリズム（暗号化アルゴリズムにおいて暗号化キーワードを復号化キーワードから計算でき、その逆も可能なものをいう）、例えば、ＤＥＳ(Data Encryption Standard)方式を利用することとする。

【００１１】ネットワーク管理者用のコンピュータ１には、予め、光ディスク等の記録媒体を介して、イントラネットの管理情報要求を本文にした電子メールを生成するプログラムが搭載されている。そして、ネットワーク管理者が、ネットワーク管理者用のコンピュータ１から電子メールにより、管理対象コンピュータ９～１１の管理情報を要求する場合、電子メール中のメッセージは暗号化装置１ａにより暗号化されてインターネット４上に送出され、ファイアウォール５を通ってイントラネット８に到達する。イントラネット８に到達した電子メールは、ゲートウェイ６の復号化装置６ｂにより、そのメッセージが復号化される。

【００１２】また、ゲートウェイ６には、予め、光ディスク等の記録媒体に記録されたプログラムをハードディスク上等に読み込んで構成された要求検出部６ｃと情報収集部６ｄおよび情報送出部６ｅが設けられており、ゲートウェイ６は、まず、要求検出部６ｃにより、復号化装置６ｂで復号化した電子メール中のメッセージからイントラネットの管理情報要求を読み出し、次に、情報収集部６ｄにより、要求検出部６ｃで読み出したイントラネットの管理情報要求に対応してイントラネットの管理情報を収集する。

【００１３】すなわち、この情報収集部６ｄは、ＳＮＭＰマネージャ１２およびＩＣＭＰエコークライアント（図中、「ＩＣＭＰ ｅｃｈｏクライアント」と記載）１３を有し、このＳＮＭＰマネージャ１２およびＩＣＭＰエコークライアント１３により、ネットワーク管理者用のコンピュータ１に代わって、管理対象コンピュータ９～１１のＳＮＭＰエージェントおよびＩＰドライバとの通信処理を行い、ネットワーク管理情報を収集する。

【００１４】そして、ゲートウェイ６は、この情報収集部６ｄで収集して暗号化装置６ｂで暗号化したイントラネットの管理情報を、情報送出部６ｅにより、電子メール中のメッセージとしてインターネット４経由でネットワーク管理者用のコンピュータ１に返送する。ネットワーク管理者用のコンピュータ１は、ゲートウェイ６からの電子メールを受信し、復号化装置１ｂによりメッセージを復号化し、ネットワーク管理者に、イントラネットの管理情報を提供する。このようにして電子メールを利用することで、ファイアウォール５を介して接続されたイントラネット８の管理をインターネット４経由で行うことができる。

【００１５】次に、図２を用いて、このような構成のイントラネットの遠隔管理システムによるネットワーク管理の実施手順を詳細に説明する。図２は、図１におけるイントラネットの遠隔管理システムの動作手順例を示す説明図である。

【００１６】ネットワーク管理者は、ネットワーク管理者用のコンピュータ１により、管理対象のネットワークアドレスとそれに加えてＭＩＢ（Management Information Base：ネットワーク管理プロトコルでアクセスされるオブジェクトの集合）の名称とそれに対して実行する

要求（リクエスト）をＡＳＮ．１（Abstract SyntaxNotation One：コンピュータの機種に依存しない抽象的なデータ構造の記述文法）形式の命令文として作成する。尚、本メッセージの一例を後述の図４で示す。

【００１７】このメッセージを暗号化装置１ａを経由してユーザエージェント２に渡す。ユーザエージェント２は、予め定義された転送先（メッセージ転送エージェント３）にメッセージを送信する。このメッセージ転送エージェント３は、ファイアウォール５経由でイントラネット８内のメッセージ転送エージェント７にメッセージを転送し、メッセージ転送エージェント７は、ゲートウェイ６にメッセージを転送する。

【００１８】ゲートウェイ６は、復号化装置６ｂによりメッセージを復号化し、ＳＮＭＰマネージャ１２、または、ＩＣＭＰエコークライアント１３のいずれか一方を呼び出す。ＳＮＭＰマネージャ１２は、命令文をＳＮＭＰ ＰＤＵ（Protocol Data Unit：あるレイヤ内のプロトコルマシンの間で交換されるデータオブジェクト）に翻訳し、管理対象コンピュータ９～１１のＳＮＭＰエージェントへ情報の取得・設定要求を送信する。

【００１９】管理対象コンピュータ９～１１のＳＮＭＰエージェントは、情報の取得要求に対しては要求された情報を、情報の設定要求に対しては処理結果を、ＳＮＭＰＰＤＵとして、ゲートウェイ６のＳＮＭＰマネージャ１２に返信する。また、ゲートウェイ６のＩＣＭＰエークライアント１３は、管理対象コンピュータ９～１１に、ＩＣＭＰエコーリクエストメッセージを送信する。管理対象コンピュータ９～１１は、ＩＰドライバにより、ＩＣＭＰエコーリクエストメッセージを受信すると、ＩＣＭＰエコーリプライメッセージを送信元に返す。

【００２０】ゲートウェイ６は、管理対象コンピュータ９～１１からＳＮＭＰマネージャ１２またはＩＣＭＰエークライアント１３に返されたＳＮＭＰ ＰＤＵやＩＣＭＰエコーリクエストメッセージに基づき返信メッセージを作成する。尚、この返信メッセージの一例を後述の図５で示す。さらに、ゲートウェイ６は、返信メッセージを暗号化装置６ａにより暗号化し、メール転送プロトコルを利用して、メッセージ転送エージェント７、ファイアウォール５を介してネットワーク管理者のメッセージ転送エージェント３に送信する。

【００２１】メッセージ転送エージェント３は、返信メッセージをユーザエージェント２に転送し、ユーザエージェント２は、返信メッセージをネットワーク管理者用のコンピュータ１に転送する。返信メッセージは、復号化装置１ｂにより復号化される。このようにしてネットワーク管理者は、応答メッセージを得ることができる。次に、ゲートウェイ６がメッセージを受信した後の処理を、図３を用いて詳細に説明する。

【００２２】図３は、図１におけるゲートウェイのメッセージ受信後の処理例を示すフローチャートである。まず、メッセージのＳＵＢＪＥＣＴフィールド（図４における符号４１）をチェックし（ステップ２５０）、ネットワーク管理要求（「MANAGEMENT_REQUEST」）であると判定した場合、メッセージを復号化し（ステップ２６）、語彙解析（ステップ２７０）および構文解析（ステップ２８０）を行う。それぞれの処理で、受信したメッセージに誤りがない場合、次のステップを実行するが、誤りがあった場合はエラーメッセージを返送する。

【００２３】次に、ゲートウェイは、メッセージの指定によりＳＮＭＰマネージャまたはＩＣＭＰエークライアントのどちらかを呼び出す（ステップ２９０）。ＳＮＭＰマネージャは、命令文（図４における符号４２，４３）をＳＮＭＰＰＤＵに翻訳し、管理対象のコンピュータのＳＮＭＰエージェントに、情報の取得・設定要求を送信する（ステップ３１０）。ＳＮＭＰエージェントは、情報の取得要求（「GetRequest」）に対しては要求された情報（図５における符号５２）を、また、情報の設定要求（「SetRequest」）に対しては処理結果（図５における符号５３）を、ＳＮＭＰ ＰＤＵとして返信する。

【００２４】また、ＩＣＭＰエークライアントは、管理対象のコンピュータにＩＣＭＰエコーリクエストメッセージ（図４における符号４４：「ping 9.1.2.8」）を送信する（ステップ３００）。管理対象のコンピュータのＩＰドライバは、ＩＣＭＰエコーリクエストメッセージ（ｐｉｎｇ）を受信すると、ＩＣＭＰエコーリプライメッセージ（図５における符号５４：「9.1.2.8 is alive」）を送信元に返す。ここで、もしターゲットのＩＰドライバが起動していない場合、あるいはネットワークの障害が発生した場合、ＩＣＭＰエコーリプライメッセージは返らない。この場合、ＩＣＭＰエークライアントはタイムアウトエラーをゲートウェイに通知する。

【００２５】さらに、ゲートウェイは、ＳＮＭＰマネージャまたはＩＣＭＰエークライアントから返されたＳＮＭＰ ＰＤＵやＩＣＭＰエコーリプライメッセージを人間が読める情報に翻訳し（ステップ３２０）、後述の図５に示す返信メッセージを作成する。そして、作成した返信メッセージを、暗号化装置で暗号化し（ステップ３３０）、メール転送プロトコルを利用してネットワーク管理者のメッセージ転送エージェントに送信する（ステップ３４０）。

【００２６】このようにして、ゲートウェイから送信された返信メッセージは、ユーザエージェント経由でメッセージ転送エージェントからネットワーク管理者のコンピュータに転送され、さらに、復号化装置により復号化され、ネットワーク管理者は、応答メッセージを得ることができる。

【００２７】図４は、図１のネットワーク管理者用のコンピュータから送出された電子メールの具体例を示す説

明図である。本メッセージにおいて、４１はヘッダ部を、４２はＳＮＭＰ Ｇｅｔリクエストを、４３はＳＮＭＰ Ｓｅｔリクエストを、４４はＩＣＭＰエコーリクエストを表す。ヘッダ部のＳＵＢＪＥＣＴフィールドの値には予め取り決めておいた「ネットワーク管理要求」を意味する文字列が設定されている。

【００２８】図５は、図１のゲートウェイから送出された電子メールの具体例を示す説明図である。本例は、図１のゲートウェイから送出された返信メッセージであり、５１はヘッダ部を、５２～５４はそれぞれ図４のＳＮＭＰ Ｇｅｔリクエスト４２、ＳＮＭＰ Ｓｅｔリクエスト４３、ＩＣＭＰエコーリクエスト４４に対応する応答文である。この返信メッセージは、図１におけるゲートウェイ６の暗号化装置６ａにより暗号化され、メール転送プロトコルでネットワーク管理者のメッセージ転送エージェントに送信される。

【００２９】以上、図１～図５を用いて説明したように、本実施例のイントラネットの遠隔管理システムでは、ネットワーク管理者は、電子メールを利用し、イントラネット内に設置されたゲートウェイに命令文を送信して、イントラネット上のコンピュータの情報の問い合わせ・設定を行い、その実行結果を電子メールにて受け取る。このように、ファイアウォールを透過可能なプロトコルである電子メールを利用して、インターネット経由でイントラネットの遠隔管理を行なうことにより、ネットワーク管理コストの削減を図ることができる。

【００３０】特に、既にインターネットに接続されている企業においては、セキュリティのレベルを維持しながら、専用回線の増設などの設備投資を行うことなしに、ゲートウェイの追加のみで、イントラネットの遠隔管理を行うことが可能となり、ネットワークの維持コストの低減を実現することが可能となる。

【００３１】尚、本発明は、図１～図５を用いて説明した実施例に限定されるものではなく、その要旨を逸脱しない範囲において種々変更可能である。例えば、本例では、図１に示すように、ゲートウェイ６に暗号化装置６ａや、復号化装置６ｂ、要求検出部６ｃ、情報収集部６ｄ、および情報送出部６ｅの各処理部を設けた構成としたが、これらの各処理部をイントラネット８内に設ける構成であれば、この構成に限定されるものではない。

【００３２】

【発明の効果】本発明によれば、インターネット経由で、ファイアウォールが設けられたイントラネットの遠隔管理が可能となり、ネットワーク管理コストの削減を図ることができる。

【図面の簡単な説明】

【図１】本発明のイントラネットの遠隔管理システムの構成の一実施例を示すブロック図である。

【図２】図１におけるイントラネットの遠隔管理システムの動作手順例を示す説明図である。

【図３】図１におけるゲートウェイのメッセージ受信後の処理例を示すフローチャートである。

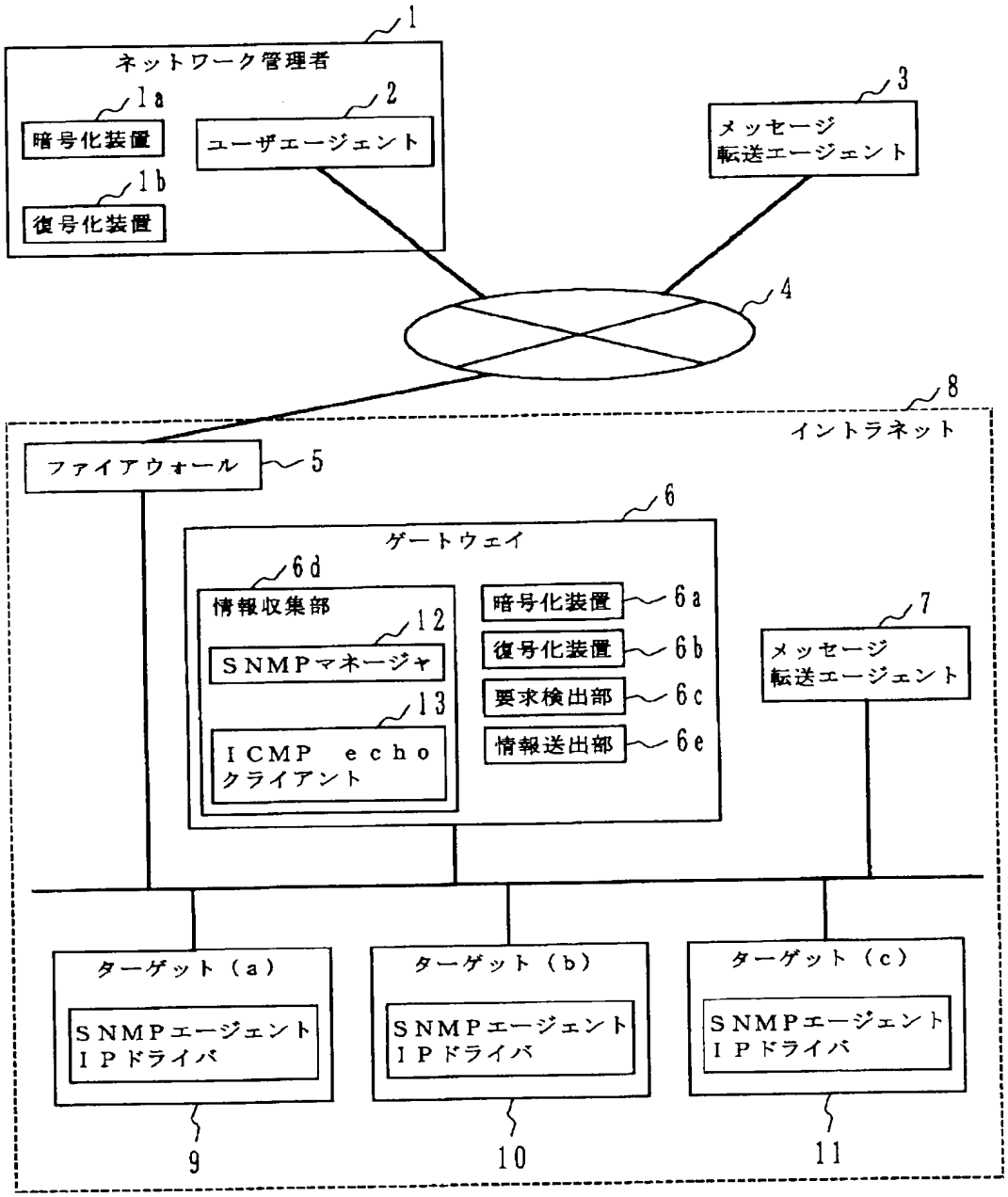
【図４】図１のネットワーク管理者用のコンピュータから送出された電子メールの具体例を示す説明図である。

【図５】図１のゲートウェイから送出された電子メールの具体例を示す説明図である。

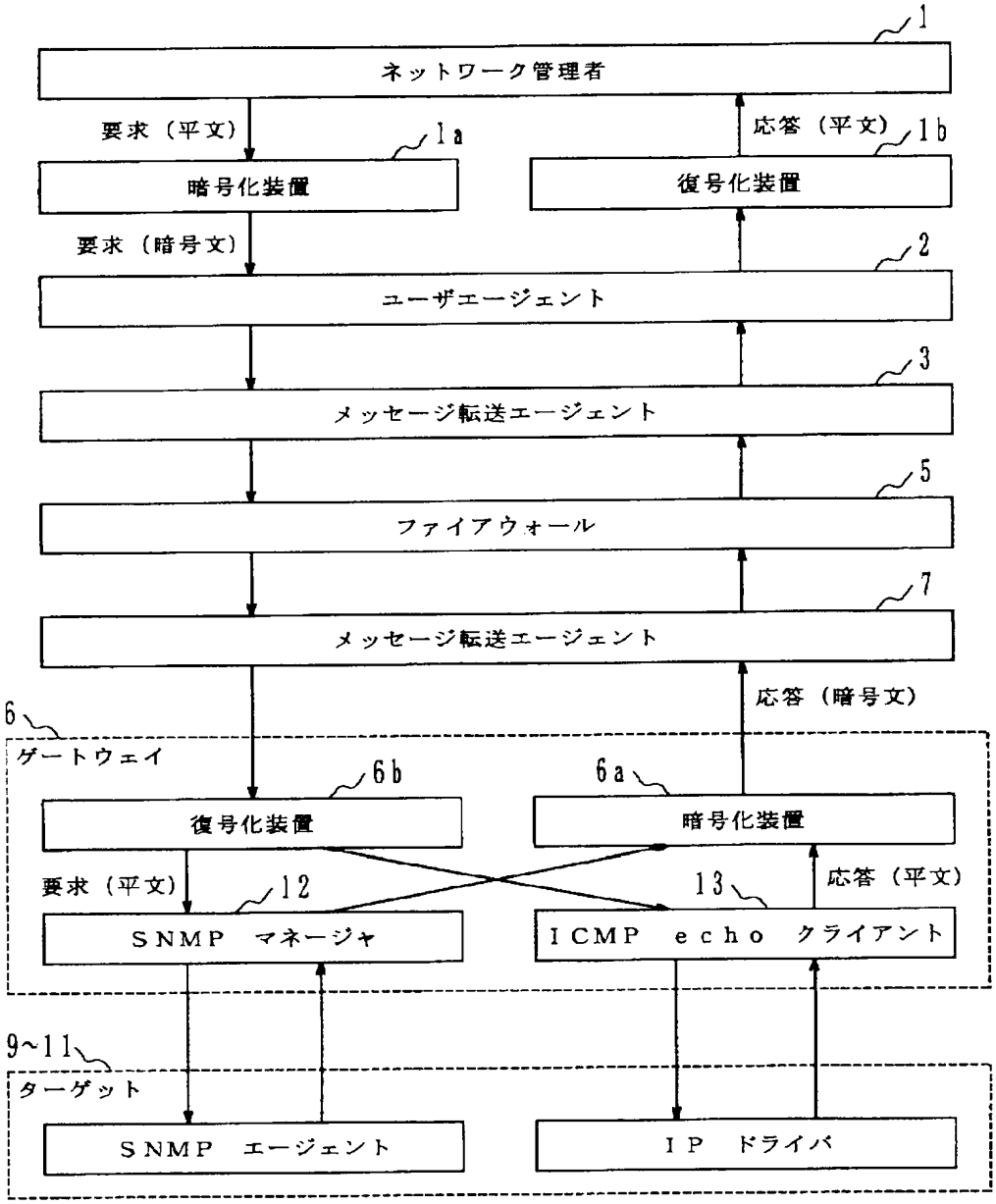
【符号の説明】

１：ネットワーク管理者用のコンピュータ、１ａ：暗号化装置、１ｂ：復号化装置、２：ユーザエージェント、３：メッセージ転送エージェント、４：インターネット、５：ファイアウォール、６：ゲートウェイ、６ａ：暗号化装置、６ｂ：復号化装置、６ｃ：要求検出部、６ｄ：情報収集部、６ｅ：情報送出部、７：メッセージ転送エージェント、８：イントラネット、９～１１：管理対象コンピュータ、１２：ＳＮＭＰマネージャ、１３：ＩＣＭＰエコークライアント、４１：ヘッダ部、４２：ＳＮＭＰ Ｇｅｔリクエスト、４３：ＳＮＭＰ Ｓｅｔリクエスト、４４：ＩＣＭＰエコーリクエスト、５１：ヘッダ部、５２～５４：応答文。

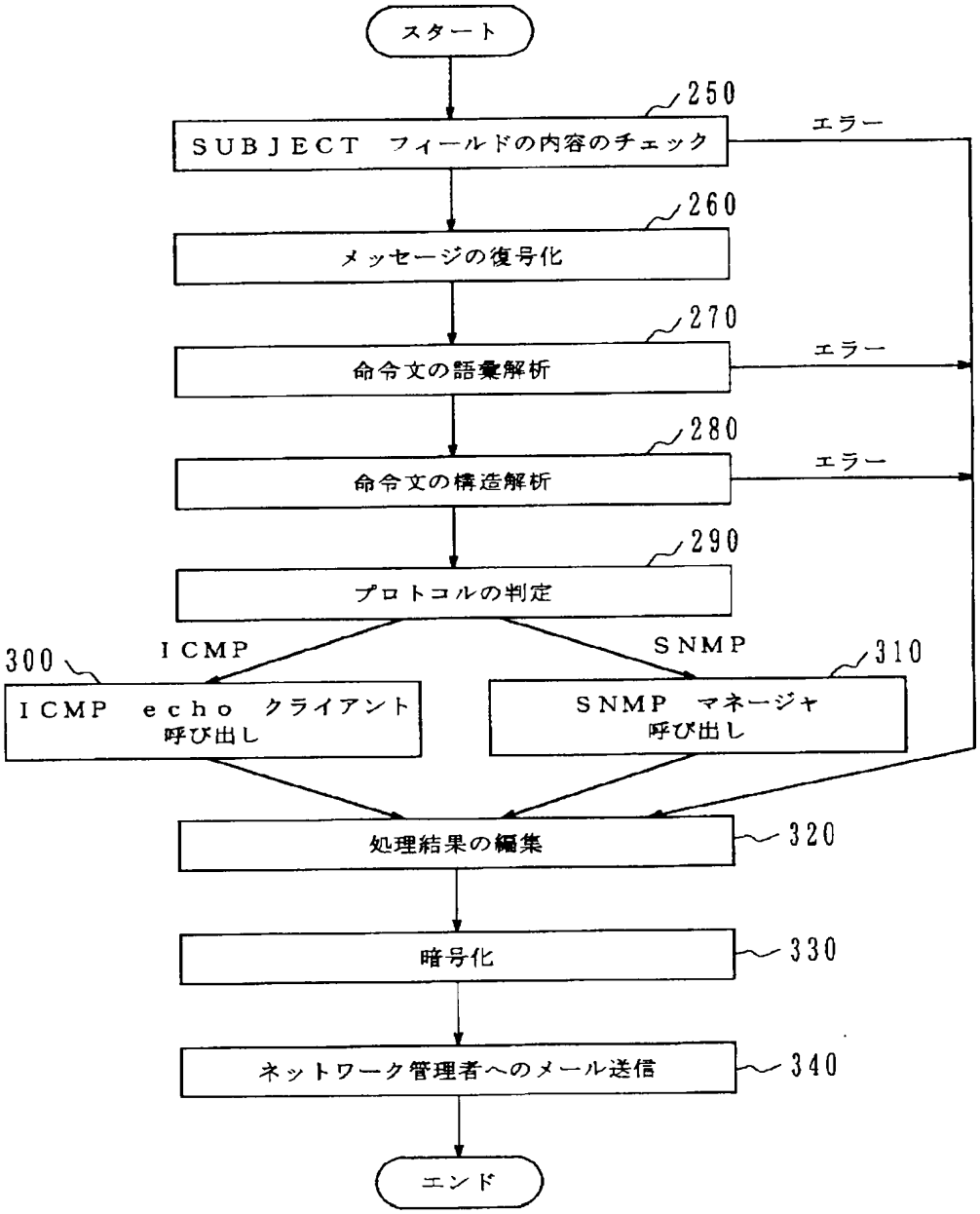
【図１】


1
ネットワーク管理者
1a
暗号化装置
1b
復号化装置
2
ユーザエージェント
3
メッセージ
転送エージェント
4
8
イントラネット
ファイアウォール
5
6
ゲートウェイ
6d
情報収集部
12
ＳＮＭＰマネージャ
13
ＩＣＭＰ　ｅｃｈｏ
クライアント
暗号化装置
6a
復号化装置
6b
要求検出部
6c
情報送出部
6e
7
メッセージ
転送エージェント
ターゲット（ａ）
ＳＮＭＰエージェント
ＩＰドライバ
ターゲット（ｂ）
ＳＮＭＰエージェント
ＩＰドライバ
ターゲット（ｃ）
ＳＮＭＰエージェント
ＩＰドライバ
9
10
11

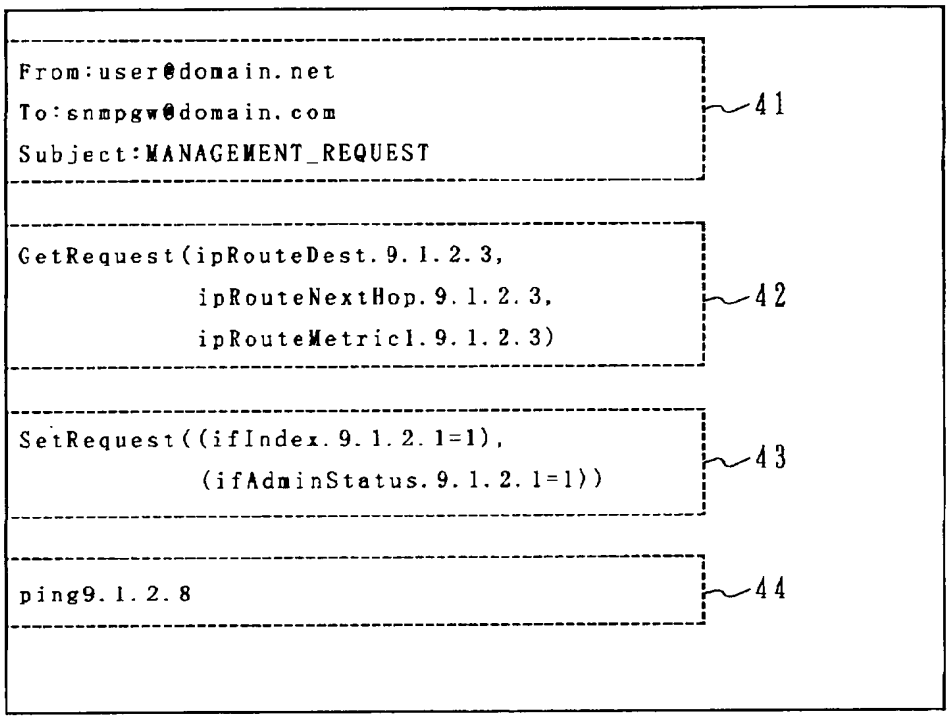
【図２】


1
ネットワーク管理者
要求（平文）
1a
暗号化装置
応答（平文）
1b
復号化装置
要求（暗号文）
2
ユーザエージェント
3
メッセージ転送エージェント
5
ファイアウォール
7
メッセージ転送エージェント
応答（暗号文）
6
ゲートウェイ
6b
復号化装置
6a
暗号化装置
要求（平文）
12
SNMP　マネージャ
13
ICMP　echo　クライアント
応答（平文）
9~11
ターゲット
SNMP　エージェント
IP　ドライバ

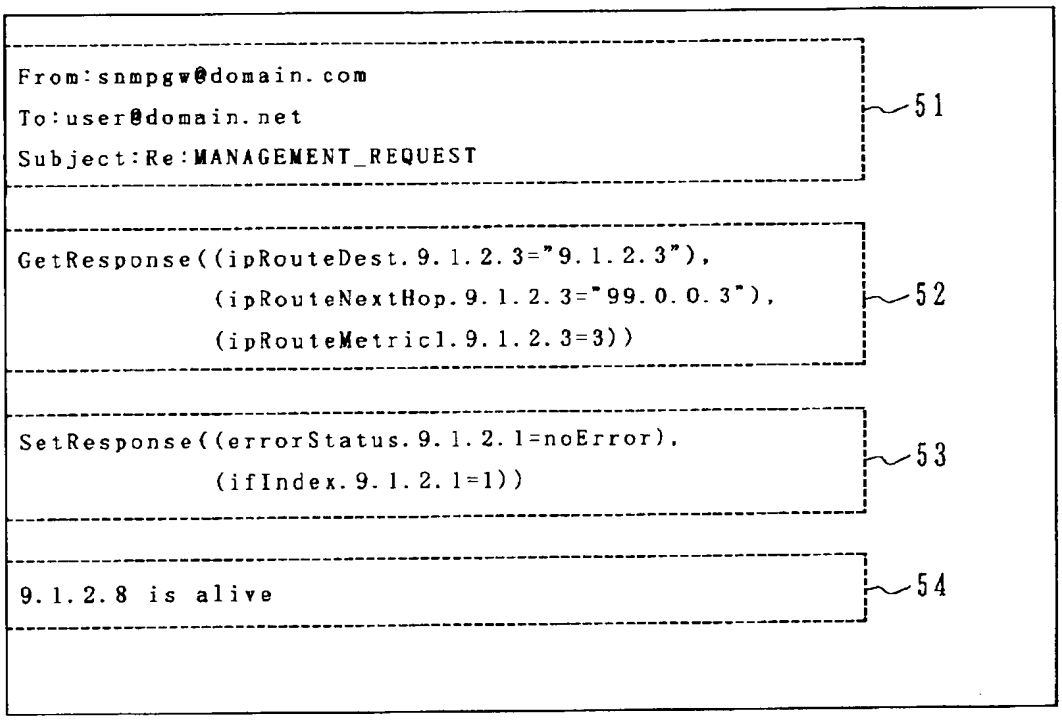
【図３】


スタート
250
ＳＵＢＪＥＣＴ　フィールドの内容のチェック
エラー
260
メッセージの復号化
270
命令文の語彙解析
エラー
280
命令文の構造解析
エラー
290
プロトコルの判定
ＩＣＭＰ
ＳＮＭＰ
300
ＩＣＭＰ　ｅｃｈｏ　クライアント
呼び出し
310
ＳＮＭＰ　マネージャ
呼び出し
処理結果の編集
320
暗号化
330
ネットワーク管理者へのメール送信
340
エンド

【図４】


From:user@domain.net
To:snmpgw@domain.com
Subject:MANAGEMENT_REQUEST
41
GetRequest(ipRouteDest.9.1.2.3,
ipRouteNextHop.9.1.2.3,
ipRouteMetric1.9.1.2.3)
42
SetRequest((ifIndex.9.1.2.1=1),
(ifAdminStatus.9.1.2.1=1))
43
ping9.1.2.8
44

【図５】


From:snmpgw@domain.com
To:user@domain.net
Subject:Re:MANAGEMENT_REQUEST
51
GetResponse((ipRouteDest.9.1.2.3="9.1.2.3"),
(ipRouteNextHop.9.1.2.3="99.0.0.3"),
(ipRouteMetric1.9.1.2.3=3))
52
SetResponse((errorStatus.9.1.2.1=noError),
(ifIndex.9.1.2.1=1))
53
9.1.2.8 is alive
54